

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

JUL - 7 2017

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Google Email Account
Michael.Yangkai@gmail.com

Case No. 1:17sw 398

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 371, 793, 794,
951 and 1956

Offense Description
Conspiracy, Gathering, transmitting or losing defense information,
Gathering or delivering defense information to aid a foreign government, Agent of a
Foreign Government, Laundering of monetary instruments

The application is based on these facts:

See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA John T. Gibbs

Sworn to before me and signed in my presence.

Date: 07/07/2017 11:00 am

City and state: Alexandria, Virginia



Applicant's signature

Stephen Green, FBI Special Agent

Printed name and title

/s/

Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The PREMISES to be searched is:

- a. This warrant applies to information associated with michael.yangkai@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.
-

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the “Provider”

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, other accounts linked to the account via cookie data, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 371, 18 U.S.C. § 793, 18 U.S.C. § 794, 18 U.S.C. § 951, and 18 U.S.C. § 1956, those violations involving Yang Kai and/or Kevin Patrick Mallory and occurring from November 23, 2011 to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Communications regarding the transmittal or receipt of classified documents or other national defense information;
- (b) Communications regarding the content of any classified documents or national defense information;
- (c) Communications regarding payment in exchange for the passing of classified documents or national defense information;
- (d) Communications with any individual residing within the United States regarding taskings at Yang Kai's behest, including the provision of non-classified information;
- (e) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- (f) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- (g) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

SEARCH PROCEDURE

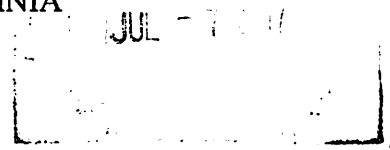
In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

1. On-site search, if practicable. Law enforcement officers training in computer forensics (hereafter computer personnel), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on-site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.
2. On-site imaging, if practicable. If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the data.
3. Seizure of digital devices for off-site imaging and search. If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.
4. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.
5. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.
6. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

7. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.
8. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN RE: SEARCH WARRANT
TO SEARCH GOOGLE ACCOUNT
MICHAEL.YANGKAI@GMAIL.COM

)
)
)
)

CASE NO. 1:17 sw **398**

Filed Under Seal

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Stephen Green, after being duly sworn, depose and state as follows:

1. I am a Special Agent with the FBI, and have been since 2012. Since 2012, I have been assigned to the Washington Field Office, Counterintelligence Division. Since October 2016, I have investigated offenses involving espionage and the unlawful retention or disclosure of classified information. I was the affiant on the affidavit in support of a criminal complaint and arrest warrant, charging Kevin Patrick Mallory (hereinafter Mallory) on June 21, 2017 with making materially false statements to Federal Bureau of Investigation (FBI) agents, in violation of 18 U.S.C. § 1001, and Gathering or Delivering Defense Information to Aid a Foreign Government, in violation of 18 U.S.C. § 794. I was the affiant on the criminal search warrant affidavit regarding michael.yangkai@gmail.com on June 16, 2017. I adopt the facts contained in that criminal complaint affidavit ("the Criminal Complaint Affidavit") and that criminal search warrant affidavit ("the Criminal Search Warrant Affidavit") as true statements for this affidavit and incorporate them here.

2. For purposes of consistency, the naming conventions used in the Criminal Complaint Affidavit and Criminal Search Warrant Affidavit have been consolidated. The individual identified as Mallory in the Criminal Complaint Affidavit and as USPER1 in the

Criminal Search Warrant Affidavit will be identified as Mallory in this affidavit. The individual identified as Yang Kai in the Criminal Search Warrant Affidavit and as PRC1 in the Criminal Complaint Affidavit will be identified as Yang Kai in this affidavit.

3. This affidavit is submitted in support of an application to search the following locations or things:

- a. LinkedIn account registered to doudz@aol.com;
- b. AOL email account doudz@aol.com;
- c. **Google email account michael.yangkai@gmail.com.**
- d. Apple records associated with e-mail michael.yangkai@gmail.com.

4. Based on the facts set forth in this affidavit (and incorporating the facts contained in the Criminal Complaint Affidavit and Criminal Search Warrant Affidavit), there is probable cause that within these locations or things is evidence, more particularly described in Attachment B, of violations of federal law, including 18 U.S.C. § 371, 18 U.S.C. § 793, 18 U.S.C. § 794, 18 U.S.C. § 951, and 18 U.S.C. § 1956.

5. This affidavit is being submitted for the limited purpose of obtaining a search warrant. As a result, it does not include each and every fact observed by me or known to the government. When I assert that a statement was made by an individual, that statement is described in substance and in part, but my assertion is not intended to constitute a verbatim recitation of the entire statement. When I assert that an event occurred or a communication was made on a certain date, I mean that the event occurred or the communication was made “on or about” that date.

6. In addition to the information contained in the Criminal Complaint Affidavit and Criminal Search Warrant Affidavit, I bring to the Court’s attention the following:

Additional Statutory Authority and Definitions

7. Under 18 U.S.C. § 371, “If two or more persons conspire to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.”

8. Under 18 U.S.C. § 793(e), “[w]hoever having unauthorized possession of, access to, or control over any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted” or attempts to do or causes the same “to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it” shall be fined or imprisoned not more than ten years, or both.

9. Under 18 U.S.C. § 794(a), “Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or, if there is no jury, the court, further finds that the offense resulted in

the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.

10. Under 18 U.S.C. § 951(a), “Whoever, other than a diplomatic or consular officer or attache, acts in the United States as an agent of a foreign government without prior notification to the Attorney General if required in subsection (b), shall be fined under this title or imprisoned not more than ten years, or both.”

11. Under 18 U.S.C. § 1956(a)(2), “Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States (A) with the intent to promote the carrying on of specified unlawful activity; or (B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or (ii) to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine of not more than \$500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for not more than twenty years, or both.”

12. Pursuant to Executive Order 13526, classified information contained on automated

information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

13. C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled "Storage," regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information "shall be stored in a GSA-approved security container, a vault built to Federal Standard (FHD STD) 832, or an open storage area constructed in accordance with § 2001.53." It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things."

LinkedIn Account registered to Kevin Mallory using Email address doudz@aol.com

14. On or about February 28, 2017, open source research indicated the existence of a LinkedIn profile for Mallory. Mallory's profile listed him as a competitive intelligence and business analyst working at GlobalEx. I know from my training and experience that LinkedIn is a communications platform, similar to Facebook, that allows individuals and entities to communicate and share information.

15. During the May 24, 2017 interview with the FBI described at paragraphs 24-33 of the Criminal Complaint Affidavit, Mallory told the agents that he was first contacted by PRC2 via LinkedIn. Mallory showed the interviewing agents the LinkedIn page for PRC2. The page indicated the accounts for Mallory and PRC2 were connected as they had five mutual friends. As described in Paragraph 24 of the Criminal Complaint Affidavit, Mallory first came in contact with PRC2, whom he described as a Chinese recruiter, in February 2017. That initial contact led

to phone interviews with PRC2 where Mallory was introduced to a second person that he described as a potential client, Yang Kai.

16. I know, based on my familiarity with this investigation, and as described more fully below, that the email address doudz@aol.com is registered to Mallory. I also know that Mallory's LinkedIn account is registered in Mallory's name using that doudz@aol.com email account.

AOL email account doudz@aol.com

17. As described in the Criminal Complaint Affidavit, on or about April 21, 2017, after a return flight to the United States from Shanghai, Mallory was subjected to a U.S. Customs and Border Protection ("CBP") secondary search and interview by CBP at Chicago O'Hare Airport. During this interaction, Mallory's email address was identified as doudz@aol.com.

18. I know, based on my training and experience that Yang Kai likely maintains and uses a number of different communications facilities, including telephone, Voice over Internet Protocol (VoIP), email and social media to communicate with his contacts such as Mallory. I know that one email account that he uses to communicate is michael.yangkai@gmail.com. Through the issuance of criminal process, I have obtained a number of communications between michael.yangkai@gmail.com and doudz@aol.com. Included in these communications were emails sent to Mallory on or about February 23, 2017, in which Yang Kai requested "another short phone call with you to address several points." Several hours later, Mallory sent a message from doudz@aol.com to michael.yangkai@gmail.com stating, "So I can be prepared, will we be speaking via Skype or will you be calling my mobile device?"

Google email account michael.yangkai@gmail.com.

19. On 14 June 2017, a preservation letter was submitted to Google's Law Enforcement Request System (LERS) for email account michael.yangkai@gmail.com. The issuance of criminal process was served to Google on June 16, 2017 via LERS. The criminal process covered the period starting January 1, 2017. As described above, a number of e-mails between michael.yangkai@gmail.com and doudz@aol.com were identified. Also included in the results was an e-mail that was sent to michael.yangkai@gmail.com from a U.S. Airline with a confirmation for a flight booked in Mallory's name.

20. Along with the e-mails, account registration information for michael.yangkai@gmail.com was provided in the response to criminal process. The michael.yangkai@gmail.com account was created on November 23, 2011. Based on the interactions between the michael.yangkai@gmail.com account with Mallory, as well as my training and experience, I believe that it is likely that the michael.yangkai@gmail.com account has been used to contact other unknown individuals in violation of 18 U.S.C. § 371, 18 U.S.C. § 793, 18 U.S.C. § 794, 18 U.S.C. § 951, or 18 U.S.C. § 1956. Included in Google's response to the issuance of criminal process, discussed above, a series of messages on or about March 7, 2017 revealed Mallory requested Yang Kai prepare a mobile phone for Mallory with Mallory's preference being an Apple phone. An e-mail was sent on or about March 8, 2017 from an Apple.com e-mail account to Yank Kai's michael.yangkai@gmail.com address. Included with that e-mail was a receipt for an Apple Iphone 7 with IMEI number 35917807506. In addition, during the May 24, 2017 interview with the FBI, Mallory told the interviewing agents that he received a brand new iPhone 7 from "them," who, based on the discussion, refers to Yank Kai and PRC3. Mallory said it was provided as a way to communicate with "them."

21. As described in paragraph 28 of the Criminal Complaint Affidavit, Mallory told

the interviewing agents that Yang Kai ultimately provided him with a communications device that he could use to communicate with Yang Kai. Mallory advised that he suspected that Yang Kai was an intelligence agent with the People's Republic of China because the type of tradecraft that Yang Kai employed would be consistent with a person who was in intelligence agent. As described in paragraphs 34-43 of the Criminal Complaint Affidavit, Mallory ultimately provided documents, comprising national defense information, to Yang Kai that were classified at either the Top Secret or Secret level. Mallory also discussed bringing "the remainder of the documents I have," in the future. Mallory also discussed getting Yang Kai to pay him using a fake name.

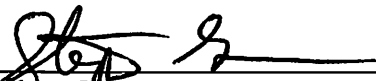
Conclusion

22. Based on the foregoing (and incorporating the information in the Criminal Complaint Affidavit and Criminal Search Warrant Affidavit), there is probable cause to believe that evidence of violations of federal law, including 18 U.S.C. §§ 371, 793(e), 794(a), 951, and 1956, more particularly described in Attachment B, will be found in the following locations and things:

- a. LinkedIn account registered to doudz@aol.com;
- b. AOL email account doudz@aol.com;
- c. **Google email account michael.yangkai@gmail.com.**
- d. Apple records associated with e-mail michael.yangkai@gmail.com.


Wherefore, I request the issuance of a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

FURTHER THIS AFFIANT SAYETH NOT.



Stephen Green
Special Agent
Federal Bureau of Investigation
Washington, D.C.

Subscribed and sworn to before me
on July 7, 2017.



/s/
Theresa Carroll Buchanan
United States Magistrate Judge
THE HONORABLE THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE